IBM

C2150-620 Exam

IBM Security Network Protection (XGS) V5.3.2 System Administration Exam

Thank you for Downloading C2150-620 exam PDF Demo

You can Buy Latest C2150-620 Full Version Download

https://www.certkillers.net/Exam/C2150-620

Version: 9.0

Question: 1

A System Administrator has been seeing a lot of SSLv2-Weak_Cipher attacks reported on the network and wants to increase the severity of the events.
How can this be accomplished?

A. Modify the Threat Level of the signature.
B. Create an Incident in SiteProtector for SSLv2_Weak Cipher.
C. Modify the Event Log response for the Intrusion Preventions Object.
D. increase the X-Force Protection Level for the Intrusion Prevention Object.

Answer: D

Explanation:
What do the various Protection Levels in the X-Force Virtual Patch and Trust X-Force Defaults mean?
Answer: For Security Network IPS (GX) sensors, there is an X-Force Virtual Patch policy that is used to determine which signatures are enabled by default (this feature is enabled by default but can be disabled). On Security Network Protection (XGS) sensors, this same Protection Level can be specified for each IPS Object in the Intrusion Prevention Policy.
Note: Intrusion Prevention Object – Threat level protection
X-Force Virtual Patch Protection Levels
Do not enable any signatures by default. This option is for a user that wants complete control over which signatures get enabled.
The moderate policy enables most attack events for a good level of security protection with minimal chance of false alarms. The moderate policy is designed for users who intermittently monitor security events and minimally manage the IPS configuration.
The aggressive policy enables a high percentage of attack events for a high level of security protection with a chance of false alarms. The aggressive policy is designed for users who perform testing and tuning before IPS deployment, and who closely monitor security events and occasionally fine-tune the IPS configuration.
The paranoid policy enables almost all attack events (including events from the latest XPUs) for a very high level of security protection with significant chance of false alarms. The paranoid policy is designed for users who perform considerable testing and tuning before IPS or XPU deployment, and who closely monitor security events and frequently fine-tune the IPS configuration.
References: http://www-01.ibm.com/support/docview.wss?uid=swg21701441

Question: 2

A System Administrator wants to configure an XGS so that when the SSH_Brute_Force security event is triggered against machine Server1, any further traffic from the source IP address contained in the security event alert is dropped for a timed period.
How should the System Administrator configure the XGS to perform this?

A. Edit the properties of the SSH_Brute_Force security event and create a quarantine response to block the source IP.
B. Create a Network Access policy object to drop all traffic from the source IP contained in the security event alert to Server1.
C. Create a Network Access policy object with a quarantine rule to block the source IP when the security event is triggered against Server1.
D. Create an IPS Filter policy object for the SSH_Brute_Force security event with a Victim address of Server1 and a quarantine response to block the source IP

Answer: C

Explanation:
Question
Why are some events allowed after setting a block response?
Cause
Most network attacks are carried out in a single packet or in several packets that are reconstructed into a single "session." For these attacks, the Block response in the XGS Intrusion Prevention policy is appropriate to use, and is translated into a block packet response and/or into a block connection response.
Certain events, however, are classified as "non-sequitur." Non-sequitur events are events that require a succession of packets to occur before the signature is triggered. For example, a port scan signature may require a succession of ten port probes before the signature would trigger. In this case, many of the offending "packets" would have already passed through the system.
Answer
For these types of signatures, you must set the Quarantine response in addition to the Block response under the Default Repository > Shared Objects > Intrusion Prevention > select signature > Edit > enable the quarantine response under the Quarantine tab > Save. The quarantine response blocks the offending IP for a period of time, ensuring that the remaining probes do not get through. The standard block packet or drop connection responses (set by the Block response) are ineffective in stopping this kind of activity when not used in conjunction with Quarantine.
List of non-sequitur events include SSH_Brute_Force.
References: http://www-01.ibm.com/support/docview.wss?uid=swg21687475

Question: 3

A System Administrator is preparing to manage an XGS appliance using the SiteProtector System.
Which three management actions can be performed? (Choose three.)

A. Apply a snapshot.
B. Restart the appliance.
C. Configure Static Routes.
D. Create a Firmware backup.
E. Manage the Appliance SSL Certificate.
F. Change the Flexible Performance Level.

Answer: A,D,E

Question: 4

A Security Administrator wants to enable a block page to alert users when they attempt to access HTTP websites that are blocked due to a Network Access policy (NAP) rule.
How should the Administrator achieve this?

A. Add a NAP rule with an action of Drop.
B. Add a NAP rule with an action of Reject.
C. Add a NAP rule that has an action of Do Not inspect and then set the response object to Block Page.
D. Add a NAP rule with an action of Reject (Authenticate) and then create a special user group that has default action of Block HTTP.

Answer: C

Question: 5

The System Administrator has discovered the XGS device is overloaded and is dropping legitimate traffic.
Which setting is likely responsible for this behavior?

A. Unanalyzed policy configuration
B. TCP resets- TCP reset interface
C. Fail Closed hardware bypass mode
D. LogDB response enabled on NAP rules

Answer: A

Thank You for trying C2150-620 PDF Demo

To Buy Latest C2150-620 Full Version Download visit link below

https://www.certkillers.net/Exam/C2150-620

Start Your C2150-620 Preparation

[Limited Time Offer] Use Coupon "CKNET" for Further discount on your purchase. Test your C2150-620 preparation with actual exam questions.